PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-152490
(43)Date of publication of application : 24.05.2002

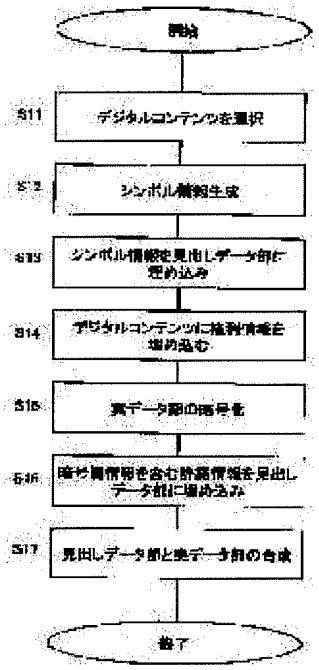
(51)Int.Cl. H04N 1/387
G06T 1/00
G09C 5/00
G10K 15/02
G10L 11/00
G10L 19/00
H04L 9/08
H04N 7/08
H04N 7/081
H04N 7/16

(21)Application number : 2000-342753
(22)Date of filing : 10.11.2000

(71)Applicant : FUJITSU LTD
(72)Inventor : HIRANO HIDEYUKI
HASHIMOTO SHINJI
HATTORI MORINORI
MOCHIZUKI SHIGETOSHI

(54) DATA OPERATING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data operating method which prevents infringements of copyrights by encoding and distributing digital contents, and readily grasps what kind of contents the digital contents included in data have.
SOLUTION: Symbol information symbolized so as to visually or aurally recognize contents of digital contents to be distributed is generated (step S12), the symbol information is embedded in a header data (step S13), the digital contents are encoded (step S15), permission information containing information on a contents key is embedded in the header data as digital watermarking (step S16), and a true data and the header data with the permission information are composited for distribution (step S17).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－152490
（P2002－152490A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		５Ｂ０５７
Ｇ０６Ｔ　1/00	５００	Ｇ０６Ｔ　1/00	５００Ｂ	５Ｃ０６３
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｃ０６４
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		５Ｃ０７６
Ｇ１０Ｌ　11/00		Ｈ０４Ｎ　7/16	Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数10　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2000－342753(P2000－342753)

(22)出願日　平成12年11月10日(2000.11.10)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

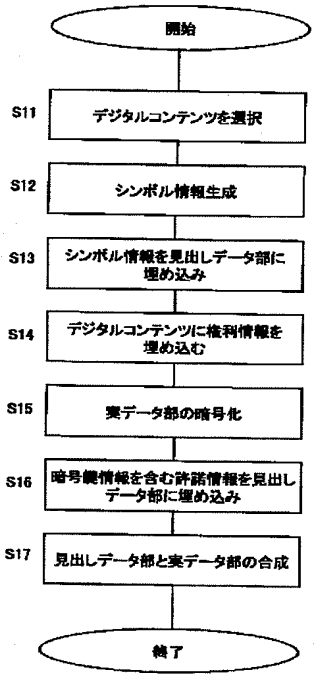
(72)発明者　橋本　晋二
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100094145
弁理士　小野　由己男　（外２名）

最終頁に続く

(54)【発明の名称】　データ運用方法

(57)【要約】
【課題】　デジタルコンテンツを暗号化して配布することで著作権の侵害を防止するとともに、データ中に含まれているデジタルコンテンツがどのような内容であるかを把握することが容易であるようなデータ運用方法を提供する。
【解決手段】　配布を行うデジタルコンテンツの内容を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を生成し（ステップＳ１２）、シンボル情報を見出しデータ部に埋め込み（ステップＳ１３）、デジタルコンテンツを暗号化し（ステップＳ１５）、コンテンツ鍵の情報を含む許諾情報を電子透かしとして見出しデータ部に埋め込み（ステップＳ１６）、実データ部と許諾情報付見出しデータ部とを合成して配布する（ステップＳ１７）。



1

【特許請求の範囲】

【請求項１】配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、前記デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

【請求項２】前記見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその属性を視覚的に認識できるようにシンボル化された１つ以上の画像シンボルデータを、１つの画像データ内に合成してなる、請求項１に記載のデータ運用方法。

【請求項３】配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成する際に前記付属データ部を同時に合成して合成データを作成してこれを配布するデータ運用方法。

【請求項４】前記利用制限情報は、前記許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックである、請求項３に記載のデータ運用方法。

【請求項５】配布を行うデジタルコンテンツを暗号化した実データ部と、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部に、前記見出しデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部と、を合成して配布される合成データから付属データ部を分離し、前記付属データ部を復号化して利用制限情報を取り出し、前記利用制限情報に基づいて前記許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、前記許諾情報から前記デジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用者に利用させるデータ運用方法。

2

【請求項６】配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部からハッシュ関数を用いて生成されたハッシュ値を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布することを特徴とするデータ運用方法。

【請求項７】配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、前記デジタルコンテンツのコンテンツ情報と、前記所定の連絡先情報とを、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布することを特徴とするデータ運用方法。

【請求項８】配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成する際に、前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

【請求項９】配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情

報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、
前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成する際に、前記デジタルコンテンツの利用者の生体情報に基づいて生成された生体テンプレート情報を前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。
【請求項１０】前記生体テンプレート情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、請求項９に記載のデータ運用方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データ運用方法に関し、特に、デジタルコンテンツを暗号化して配布する際のデータ運用情報に関する。
【０００２】
【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピー（登録商標）ディスク（ＦＤ）、ミニディスク（ＭＤ）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。
【０００３】また、インターネットやＣＡＴＶ、その他のネットワークなどを通じて配布される静止画像データ、動画像データ、音声データ、音楽データを含む電子化データについても同様にして不正コピーが頻繁に行われ、著作権者の利益が損なわれている。
【０００４】このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの暗号化された実データを配布することが行われる。
【０００５】たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのＣＰＵ識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。
【０００６】コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。
【０００７】ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。
【０００８】この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。
【０００９】
【発明が解決しようとする課題】上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。
【００１０】また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツとその許諾情報とを別々に記録媒体に格納しておく必要がある。したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを利用することができなくなり、再度許諾情報を入手する手順が必要となる。
【００１１】また、図書館の写本、美術館所蔵品などを写真やスキャナなどで画像データとして取り込み、これをユーザに利用させる場合、画像データが完全に暗号化されていると許諾情報のやりとりを行う前に、ユーザ側で所望の画像データを特定することが困難である。したがって、画像の一部がユーザ側で確認でき、かつ不正に流用されることがないように運用することが望ましい。
【００１２】静止画像、動画像などの画像データのみならず、音声データや音楽データなどを暗号化して配布する場合においても、どのようなデジタルコンテンツが含まれているかを視覚的または聴覚的に確認できるようにしておくことで、利用者にとって便利になる。
【００１３】本発明は、デジタルコンテンツを暗号化して配布することで著作権の侵害を防止するとともに、データ中に含まれているデジタルコンテンツがどのような内容であるかを把握することが容易であるようなデータ運用方法を提供する。
【００１４】
【課題を解決するための手段】本発明に係るデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実

データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布する。

【００１５】ここで、見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその内容を視覚的に認識できるようにシンボル化された１つ以上の画像シンボルデータを１つの画像データ内に合成して構成することができる。

【００１６】また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、実データ部と許諾情報付見出しデータ部とを合成する際に付属データ部を同時に合成して合成データを作成してこれを配布する。

【００１７】このとき、利用制限情報として、許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックを用いることができる。また、利用制限情報は、デジタルコンテンツを利用可能な利用期限または利用回数に基づくものとすることができる。

【００１８】さらに、利用制限情報は、デジタルコンテンツの利用者の個人情報を暗号鍵として暗号化することができる。この利用制限情報を暗号化する際の暗号鍵は、利用者によって予め設定されたパスワードとすることができ、合成データが記録される記録媒体に固有の識別情報とすることもでき、利用者の生体情報を用いることも可能である。

【００１９】本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部と、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部に、デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部とを合成して配布される合成データから付属データ部を分離し、付属データ部を復号化して利用制限情報を取り出し、利用制限情報に基づいて許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、許諾情報からデジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて実データ部を元のデジタルコンテンツに復号化して利用者に利用させる。

【００２０】また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部からハッシュ関数を用いて生成されたハッシュ値を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成してこの合成データを配布する。

【００２１】さらに、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、記録される記録媒体に固有の識別情報とを視覚的または聴覚的に認識不能な電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布する。

【００２２】また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、デジタルコンテンツを再生するための情報機器に特定の動作をさせる制御コードとを視覚的または聴覚的に認識不能な電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布する。

【００２３】さらに、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、デジタルコンテンツのコンテンツ情報と、所定の連絡先情報とを、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成し、この合成データを配布する。

【００２４】また、本発明のデータ運用方法は、配布を

行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成した合成データを作成する際に、デジタルコンテンツを登録しているサーバの記録場所情報を、合成データ中に保持させ、この合成データを配布する。

【００２５】ここで、デジタルコンテンツを登録しているサーバの記録場所情報を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことができる。

【００２６】さらに、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成して合成データを作成する際に、デジタルコンテンツの利用者の生体情報に基づいて生成された生体テンプレート情報を、合成データ中に保持させ、この合成データを配布する。

【００２７】ここで、生体テンプレート情報を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことができる。また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成して合成データを作成し、この合成データを配布するものであって、デジタルコンテンツの著作権情報や版権情報を含む権利情報を、デジタルコンテンツ中に電子透かしとして埋め込む。

【００２８】この場合、デジタルコンテンツに要求されるデータ品質レベルとセキュリティレベルとに基づいて、デジタルコンテンツ中に埋め込む電子透かしの形態と暗号化レベルを決定するように構成できる。

【００２９】また、デジタルコンテンツ中への電子透かしの埋め込み方式と、見出しデータ部への電子透かしの埋め込み方式が異なる構成とすることができる。

【００３０】【発明の実施の形態】〔発明の概要〕図１に本発明の概要構成を示す。

【００３１】コンテンツ提供者１は、デジタルコンテンツの著作者、版権者などであり、運用を行うデジタルコンテンツ１１をコンテンツ管理者２に提供する。コンテンツ管理者２は、コンテンツ提供者１から提供されるデジタルコンテンツ１１を運用するために暗号化し、暗号化する際の暗号鍵として用いたコンテンツ鍵を管理するとともに、このデジタルコンテンツ１１を利用するユーザの利用者情報を管理する。

【００３２】コンテンツ利用者３は、コンテンツ管理者２が管理しているデジタルコンテンツを利用したい場合には、利用者情報１４をコンテンツ管理者２に送信する。コンテンツ管理者２は、コンテンツ利用者３から送信された利用者情報１４を管理するとともに、この利用者情報１４に基づいて許諾情報１３を作成し、デジタルコンテンツを暗号化した実データ部１５と許諾情報１３とを含む合成データ１２をコンテンツ利用者３に送信する。

【００３３】このとき、コンテンツ管理者２はデジタルコンテンツ１１の属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を用いて見出しデータ部１６を作成する。デジタルコンテンツ１１を暗号化する際に用いたコンテンツ鍵を利用者情報１４によって暗号化して許諾情報１３を作成し、これを見出しデータ部１６に電子透かしとして埋込んだ許諾情報付見出しデータ部を作成する。さらに、デジタルコンテンツを暗号化した実データ部１５と許諾情報付見出しデータ部とを合成してコンテンツ利用者３に送信する。

【００３４】合成データ部１２は、図２に示すように、見出しデータ部１６と、暗号化された実データ部１５が合成されたデータ構成となる。許諾情報を電子透かしとして見出しデータ部１６に埋め込む際の埋込ロジックとして、コンテンツ管理者２側とコンテンツ利用者３側との間で予め設定されたものを用いる場合は、このようなデータ構成とすることができる。

【００３５】コンテンツ利用者３側において、複数の埋込ロジックに対応して電子透かしを復号化することが可能な場合には、コンテンツ管理者２が合成データ１２中に埋込ロジックに関する情報を含ませて送ることが必要となる。この場合、図３に示すように、埋込ロジックに関する情報を付属データ部１７に格納して、見出しデータ部１６、実データ部１５とともに合成データ１２を作成することが考えられる。

【００３６】付属データ部１７には、埋込ロジックに関する情報の他に、許諾情報が電子透かしとして見出しデータ部に埋め込まれている位置と電子透かしのサイズに関する位置情報、デジタルコンテンツの使用期限や使用回数制限などに関する使用制限情報などを格納することも可能である。また、この付属データ部１７に格納され

る情報を暗号化することが考えられ、たとえば、許諾情報を生成した際に用いた利用者情報１４で暗号化するように構成できる。

【００３７】さらに、許諾情報を暗号化する際に用いた暗号鍵である利用者情報１４は、見出しデータ部１６に電子透かしとして埋め込むことも可能であり、付属データ部１７に格納することも可能である。この場合には、コンテンツ利用者３がデジタルコンテンツを再生する前に、本人認証を行うことが可能となり、不正利用を防止することが可能となる。

【００３８】なお、コンテンツ提供者１とコンテンツ管理者２は同一であってもよい。

〔コンテンツ管理者〕コンテンツ管理者２側の概略構成を示す機能ブロック図を図４に示す。

【００３９】このコンテンツ管理者２側では、運用を行うコンテンツを管理するコンテンツ管理部２１、所定のコンテンツ鍵を用いてデジタルコンテンツを暗号化するコンテンツ暗号化部２２、コンテンツ鍵を管理するコンテンツ鍵管理部２３、コンテンツ利用者３の利用者情報を取得してこれを管理する利用者情報管理部２４、利用者情報管理部２４で管理している利用者情報情報に基づいてデジタルコンテンツの利用許諾情報を作成しこれを管理する許諾情報管理部２５、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、この見出しデータ部に許諾情報を電子透かしとして埋め込む見出しデータ作成部２６、コンテンツ鍵を用いてデジタルコンテンツを暗号化した実データ部と許諾情報付見出しデータ部とを合成する合成データ作成部２７などを備えている。

【００４０】〔コンテンツ利用者〕コンテンツ利用者３側の概略構成を示す機能ブロック図を図５に示す。このコンテンツ利用者３側では、使用しているハードディスクドライブの識別番号、コンピュータに搭載されているＣＰＵの識別番号、その他の利用者固有の識別情報を管理する利用者情報管理部３１、コンテンツ管理者２からの合成データを取得するための合成データ取得部３２、取得した合成データのうち見出しデータ部を表示するための見出しデータ表示部３３、許諾情報付見出しデータ部から許諾情報を分離する許諾情報抽出部３４、抽出した許諾情報を復号化してコンテンツ鍵を再生するコンテンツ鍵復号部３５、復号化されたコンテンツ鍵を用いて暗号化コンテンツを復号化するコンテンツ復号部３６、復号化したデジタルコンテンツを動作させるコンテンツ動作部３７などを備えている。

【００４１】〔コンテンツ配布〕コンテンツ管理者２側において、デジタルコンテンツを配布する際の手順について、図６に示すフローチャートに基づいて説明する。

【００４２】ステップＳ１１では、配布を行う合成データ１２中に格納するデジタルコンテンツを選択する。このデジタルコンテンツは、静止画像データ、動画像データ、音声データ、音楽データおよびこれらを複合的に含む電子化データであり、たとえば、JPEG、TIFF、GIF、ビットマップ、その他の形式による画像データを選択でき、また、MP3、WAV、その他の形式による音声データを選択することが可能である。

【００４３】ステップＳ１２では、選択した各デジタルコンテンツについて、その属性を視覚的または聴覚的に認識できるようにしたシンボル情報を作成する。このシンボル情報は、そのデジタルコンテンツのデータ形式に対応するアイコンを当てはめることが可能である。

【００４４】たとえば、各シンボル情報はアイコンのような画像データを用いることが可能であり、たとえば、図８のデータテーブルに示すように、データ種別、シンボル情報、デジタルコンテンツのデータ形式に基づく拡張子をそれぞれ対応させて定義しておくことができる。

【００４５】ステップＳ１３では、各デジタルコンテンツに対応して作成したシンボル情報が埋め込まれた見出しデータ部１６を作成する。見出しデータ部１６は、たとえば、画像データとして生成された各デジタルコンテンツのシンボル情報が、１つの画像データ中に埋め込まれた構成とすることができる。また、音声データとした場合には、各デジタルコンテンツのシンボル情報が、順次連結された１つの音声データとすることも可能である。また、画像データ中に埋め込まれたシンボル情報が、音声データを伴うように構成することも可能である。

【００４６】ステップＳ１４では、合成データ１２中に格納される各デジタルコンテンツに権利情報の埋込処理を行う。この権利情報は、デジタルコンテンツの著作権情報や出版権情報などを示すものであり、必要に応じてデジタルコンテンツ中への埋込処理が行われる。権利情報のデジタルコンテンツへの埋込処理は、不可視または不可聴の電子透かしとして埋め込むことが可能であり、可視的または可聴的な電子透かしとすることも可能である。

【００４７】ステップＳ１５では、合成データ１２中に格納される各デジタルコンテンツをそれぞれ対応するコンテンツ鍵により暗号化して実データ部１５を作成する。暗号化する方法は、各種暗号法を採用することができ、特に秘密鍵暗号系による暗号化を行うことが好ましい。この場合、各デジタルコンテンツに対応してコンテンツ管理者２側でコンテンツ鍵を自動生成し、このコンテンツ鍵を用いて暗号化された実データ部の生成を行う。デジタルコンテンツ毎に異なるコンテンツ鍵を用いるように構成することも可能であり、合成データ中の各デジタルコンテンツを共通のコンテンツ鍵を用いて暗号化するように構成することも可能である。

【００４８】ステップＳ１６では、デジタルコンテンツを暗号化する際に用いたコンテンツ鍵の情報を含む許諾

情報を生成し、この許諾情報を見出しデータ１６に埋め込む。許諾情報は、デジタルコンテンツの暗号化に用いたコンテンツ鍵を、コンテンツを利用するユーザに固有の利用者情報１４を用いて暗号化したものとすることができる。このユーザに固有の利用者情報１４は、ユーザに対して予め設定されたパスワードとすることができる。また、この利用者情報１４は、ユーザがデジタルコンテンツを動作させる際に使用する情報機器の識別情報とすることができ、たとえば、パソコンに搭載されているCPUのシリアルナンバー、CD-ROM、DVD、MO、FD、HDなどドライブのシリアルナンバーが採用され得る。この場合、ユーザのパスワードまたは使用する情報機器の識別情報をコンテンツ管理者２側で登録しておき、この登録されている利用者情報１４に基づいてコンテンツ鍵を暗号化するように構成できる。

【００４９】さらに、ユーザに固有の利用者情報１４として、ユーザの生体情報を用いることが可能である。たとえば、ユーザの指紋情報、網膜情報、虹彩情報、声紋情報などを予めコンテンツ管理者２側に登録しておき、各生体情報に基づいてコンテンツ鍵を暗号化するように構成できる。たとえば、指紋情報を用いてコンテンツ鍵を暗号化する場合、予めユーザからコンテンツ管理者２側に利用者本人の指紋画像を登録してもらう。コンテンツ管理者２側では、登録されているユーザの指紋画像を分析して、指紋画像のうち端点・分岐点などのマニューシャと呼ばれる特徴点を抽出し、この特徴点情報によりコンテンツ鍵を暗号化する。

【００５０】ステップ１６では、コンテンツ鍵を利用者情報１４により暗号化した許諾情報１３を見出しデータ部１６に電子透かしとして埋め込む。この見出しデータ１６への許諾情報１３の埋め込みは、不可視または不可聴の電子透かしとして埋め込む構成とすることができ、見出しデータ１６の特定の周波数帯域に許諾情報１３を挿入する、データの一部を間引きしてここに許諾情報を挿入する、その他の方法が考えられる。

【００５１】ステップＳ１７では、見出しデータ部１６と実データ部１５とを合成して合成データ１２を作成する。見出しデータ部１６に許諾情報１３を埋め込む際の埋め込みロジックを格納する付属データ部１７を必要とする場合には、見出しデータ部１６、実データ部１５とともに付属データ部１７を合成して合成データ１２（図３参照）を作成する。

【００５２】このようにして作成された合成データ１２は、CD-ROM、DVD、光磁気ディスク（MO）、MD、フロッピーディスク、その他の記録媒体に記録されてユーザに送られるか、あるいはインターネットを通じて直接ユーザのパソコンなどの情報機器に配信され、ハードディスク上に格納される。

【００５３】〔コンテンツ利用〕配布された合成データ１２をコンテンツ利用者３側で利用する場合について、図７のフローチャートに基づいて説明する。

【００５４】ステップＳ２１では、合成データ１２から実データ部１５と見出しデータ１６とを分離する。付属データ部１７がある場合には同時にこの付属データ部１７も分離する。

【００５５】ステップＳ２２では、見出しデータ部１６に電子透かしとして埋め込まれている許諾情報１３を取り出して、この許諾情報１３からコンテンツ鍵を復号化する。許諾情報１３は見出しデータ部１６に所定の埋め込みロジックにより電子透かしとして埋め込まれており、コンテンツ管理者２とコンテンツ利用者３との間で予め決めた埋め込みロジックを使って、許諾情報１３を取り出すことが可能である。

【００５６】付属データ部１７に、電子透かしの埋め込みロジックが格納されている場合には、この付属データ部１７から埋め込みロジックの情報を取り出して、これに基づいて許諾情報１３を取り出すように構成する。電子透かしが埋め込まれている位置やサイズに関する位置情報が付属データ部１７に格納されている場合も、この位置情報を付属データ部１７から取り出してこれを利用して許諾情報１３を取り出す。

【００５７】許諾情報１３は、利用者情報１４に基づく暗号鍵によって暗号化されたものであり、利用者情報１４を用いて復号化が可能となる。利用者情報１４がパスワードである場合には、ユーザによるパスワードの入力を受け付けてこの入力パスワードを用いて許諾情報１３を復号化する。また、CPUのシリアルナンバーやメディアドライブのシリアルナンバーなどでなる情報機器の識別情報により暗号化されている場合には、現在使用している情報機器の識別情報を取得して、これに基づいて許諾情報１３を復号化する。さらに、ユーザの生体情報で暗号化されている場合には、ユーザの生体情報の入力を受け付けて、これを端点・分岐点などによる特徴点情報に解析し、この特徴点情報により復号化するように構成できる。

【００５８】ユーザから受け付けたパスワード、ユーザが現在使用している情報機器の識別情報、ユーザから受け付けた生体情報に基づく特徴点情報などが正常であれば、許諾情報１３から正当なコンテンツ鍵が復元されることとなる。

【００５９】ステップＳ２３では、復元されたコンテンツ鍵を用いて実データ部１５を復号化してデジタルコンテンツの復元を行う。復元されたデジタルコンテンツは、コンテンツ利用者３側のハードディスクやその他の記録媒体上で展開されて格納される。

【００６０】ステップＳ２４では、見出しデータ部１６に記録されているシンボル情報に基づいて、このシンボル情報に定義付けされているファイル拡張子情報を抽出して、復元されたデジタルコンテンツと関連付ける。

【００６１】ステップＳ２５では、ユーザの指示に基づ

いて、ファイル拡張子情報に関連するアプリケーションを起動し、デジタルコンテンツの利用を行う。復元されたデジタルコンテンツが実行形式のファイルである場合には、ユーザによるアプリケーションの起動を待たずに、ファイルの指定があれば自己起動するように構成できる。

【００６２】〔生体情報による認証方法〕デジタルコンテンツを利用しようとしているユーザが、正当な利用者であるか否かの認証を、ユーザの生体情報を用いて行うことが可能である。生体情報としては、前述のように、指紋情報、網膜情報、虹彩情報、声紋情報などが考えられる。ここでは、指紋情報を用いて認証を行う場合について、図９、図１０に基づいて説明する。

【００６３】ユーザの指紋情報に基づいて本人認証を行う場合には、予めユーザからコンテンツ管理者２側に利用者本人の指紋画像を登録してもらう。ステップＳ３１では、登録されているユーザの指紋画像に基づいて、検査対象となる指紋との照合を行うテンプレート情報を作成する。

【００６４】指紋画像の端点・分岐点などのマニューシャと呼ばれる特徴点情報による照合を行う場合には、登録されている指紋画像から特徴点情報を抽出してこれをテンプレート情報として登録する。

【００６５】また、登録されているユーザの指紋画像を細線化画像とし、検査対象となる指紋の二値化画像とのパターンマッチングを行う方法を用いる場合には、登録されているユーザの指紋画像から細線化画像を作成し、これをテンプレート情報とする。

【００６６】ステップＳ３２では、登録されているユーザの指紋画像から作成したテンプレート情報を見出しデータ部１６または付属データ部１７に記録する。見出しデータ部１６にテンプレート情報を記録する場合には、不可視な電子透かしとして埋め込むように構成できる。また、付属データ部１７を有するデータ構造である場合には、この付属データ部１７にテンプレート情報を格納するように構成できる。

【００６７】コンテンツ利用者３側では、図１０に示すフローチャートに基づいて本人認証動作を行う。ステップＳ４１では、コンテンツ利用者３側に設置される指紋読取装置によりユーザの指紋を読み取り、その指紋画像から検査対象となる指紋情報を取得する。前述したように、指紋の特徴点に基づいて照合を行う場合には、読み取った指紋画像からその端点・分岐点などに基づく特徴点情報を生成する。また、細線化画像とのパターンマッチングを行う場合には、読み取った指紋画像から二値化画像を生成する。

【００６８】ステップＳ４２では、見出しデータ部１６または付属データ部１７に記録されているテンプレート情報を取り出す。見出しデータ部１６にテンプレート情報が電子透かしとして記録されている場合には、所定の埋め込みロジックにより見出しデータ部１６からテンプレート情報を取り出すこととなる。

【００６９】ステップＳ４３では、検査対象となる指紋情報とテンプレート情報とを照合して本人認証を行う。特徴点情報に基づいて照合を行う場合には、検査対象となる指紋画像から得た特徴点情報と、登録されているユーザの指紋から得た特徴点情報であるテンプレートが比較され、その比較結果に基づいて本人認証が行われる。また、細線化画像による照合を行う場合には、検査対象となる指紋画像の二値化情報と、登録されているユーザの指紋から得た細線化画像とをパターンマッチングし、その結果に基づいて本人認証が行われる。

【００７０】〔コンテンツ利用情報〕利用者情報１４などのユーザに関する情報をデジタルコンテンツ内に埋め込むことで、利用状況をデジタルコンテンツ内に残すことが可能である。たとえば、配布を行う合成データ１２中のデジタルコンテンツに配布先であるユーザの利用者情報１４を埋め込むことで、最初に配布を行ったユーザの情報を残すことが可能となる。また、デジタルコンテンツの利用時にそのユーザの利用者情報１４を取得し、これをデジタルコンテンツ中に埋め込むように構成すれば、利用者の履歴を残すことができる。

【００７１】デジタルコンテンツ内に利用するユーザの指紋情報を埋め込む場合について、図１１のフローチャートに基づいて説明する。ステップＳ５１では、デジタルコンテンツを利用しようとするユーザの指紋画像情報を生成する。

【００７２】ステップＳ５２では、合成データのデジタルコンテンツ内にユーザの指紋画像情報を埋め込む。たとえば、コンテンツ管理者２側において、配布する合成データ１２中に含まれるデジタルコンテンツに、予め登録されている配布先のユーザの指紋画像情報を、不可視な電子透かしとして埋め込むことが考えられる。この場合、最初に配布を行ったユーザの指紋画像情報がデジタルコンテンツ内に埋め込まれており、不正にコピーされた場合であってもその出所を判別することが可能となる。

【００７３】また、デジタルコンテンツを利用しようとする際に、ユーザの指紋画像情報を取得し、これをデジタルコンテンツ内に埋め込むように構成することも可能である。この場合も、利用しようとするユーザの指紋画像情報を不可視な電子透かしとしてデジタルコンテンツ内に埋め込むように構成できる。この場合、不正に利用しようとした場合であっても、デジタルコンテンツに利用者の履歴情報が残ることとなり、このデータが不正に流出した経路を知ることができる。

【００７４】〔電子透かし埋め込みロジック〕前述したように、見出しデータ部１６に許諾情報１３を不可視な電子透かしとして埋め込む場合に、許諾情報１３を埋め込む際に用いた埋め込みロジックの情報を合成データ１

２内に持たせることができる。見出しデータ部１６には、許諾情報１３の他にユーザの生体情報、著作権や版権などに関する権利情報などを電子透かしとして埋め込むことが考えられ、またデジタルコンテンツ内にも、ユーザの生体情報、著作権や版権などに関する権利情報、利用期限や利用回数制限などに関する利用情報などを埋め込むことが考えられる。見出しデータ部１６と実データ部１５に含まれる電子透かしの埋め込みロジックの種別やバージョン情報をそれぞれ付属データ部１７に格納しておくことで、コンテンツ利用者３側での利用が容易となる。この動作について、図１２および図１３のフローチャートに基づいて説明する。

【００７５】ステップＳ６１では、配布する合成データ１２の見出しデータ部１６および実データ部１５のそれぞれに含まれる電子透かしの埋め込みロジックの種別データとバージョン情報を付属データ部１７に格納する。

【００７６】たとえば、見出しデータ部１６および実データ部１５で使用される埋め込みロジックを、図１４のテーブルのように定義することができる。ここでは、見出しデータ部１６で使用される埋め込みロジックの種別とバージョン情報および実データ部１５で使用される埋め込みロジックの種別とバージョン情報を順に並べて４桁の数値とし、これに基づいて埋め込みロジックを定義している。

【００７７】ステップＳ６２では、付属データ部１７に設定された埋め込みロジックにしたがって、見出しデータ部１６および実データ部１５にそれぞれ電子透かしの埋め込み処理を実行する。

【００７８】コンテンツ利用者３側において、配布された合成データ１２から電子透かしのデータを取り出す場合には、図１３のフローチャートに基づいて動作する。ステップＳ７１では、合成データ１２中の付属データ部１７から埋め込みロジックの情報を取得する。

【００７９】ステップＳ７２では、取得した埋め込みロジックの情報に基づいて、見出しデータ部１６および実データ部１５に埋め込まれた電子透かしを取り出す。取得した埋め込みロジックの情報は、前述したように、見出しデータ部１６に対する埋め込みロジックの種別とバージョン情報および実データ部１５に対する埋め込みロジックの種別とバージョン情報で構成されており、これに基づいて各電子透かしの情報を取り出すことが可能となる。

【００８０】〔実データ部のハッシュ値〕デジタルコンテンツの内容の改竄やデータの置き換え、通信中のエラーなどを検出するために、実データ部１５のハッシュ値を生成し、これを合成データ１２中に記録しておく構成とすることができる。ハッシュ値は、ハッシュ関数を用いて求められる固定長の疑似乱数であり、このハッシュ値から原文を再現することができないように、不可逆な一方方向関数により生成される。

【００８１】このような見出しデータ部１５のハッシュ値を見出しデータ部１６に埋め込む場合について、図１５および図１６のフローチャートに基づいて説明する。ステップＳ８１では、実データ部１５のデータを特定のハッシュ関数に入力しハッシュ値を生成する。ハッシュ値を求める実データ部としては、暗号化前のデジタルコンテンツのデータとすることも可能であり、コンテンツ鍵による暗号化された実データ部とすることも可能である。また、ハッシュ関数は、SHA-1やMD5、その他のものを用いることが可能である。

【００８２】ステップＳ８２では、生成された実データ部１５のハッシュ値を見出しデータ部１６に不可視な電子透かしとして埋め込む。電子透かしの埋め込みロジックは、前述したような埋め込みロジック種別およびバージョン情報で定義されたものを用いることができる。

【００８３】合成データ１２に含まれる実データ部１５のハッシュ値を求め、見出しデータ部１６に埋め込まれたハッシュ値と比較することによって、データの置き換えなどの不正があったことを検証することができる。このときの動作を図１６のフローチャートに基づいて説明する。

【００８４】ステップＳ９１では、合成データ１２中に含まれる実データ部１５のデータを特定のハッシュ関数に入力し、ハッシュ値を求める。ここでは、見出しデータ１６中に電子透かしとして埋め込まれたハッシュ値と同じハッシュ関数を用いることが必要である。

【００８５】ステップＳ９２では、合成データ１２の見出しデータ部１６に埋め込まれているハッシュ値を抽出する。ハッシュ値は、前述の埋め込みロジックに基づいて電子透かしとして見出しデータ部１６に埋め込まれており、この埋め込みロジックに基づいて抽出することで検証用のハッシュ値を取得することができる。

【００８６】ステップＳ９３では、ハッシュ関数により生成した実データ部１５のハッシュ値と、見出しデータ部１６から抽出した検証用のハッシュ値を比較して一致するか否かの検証を行う。

【００８７】このように、見出しデータ部１６に実データ部１５のハッシュ値を埋め込むことにより、合成データ１２に含まれるデジタルコンテンツが改竄されたことや不正にデータの置き換えがあったことを認識することが可能となる。

【００８８】〔サーバの記録場所情報〕配布する合成データ１２中に含まれるデジタルコンテンツを管理しているサーバの記録場所情報を合成データ１２中に含ませることができる。この場合の動作について図１７および図１８のフローチャートに基づいて説明する。

【００８９】ステップＳ１０１では、配布するデジタルコンテンツを管理するサーバの格納情報を取得する。この場合、サーバ内のデジタルコンテンツが格納されている場所を示すURLなどを格納情報として取得する。

【００９０】ステップＳ１０２では、見出しデータ部１６に不可視な電子透かしとして格納情報を埋め込む。この場合も、前述と同様にして設定された埋め込みロジックを用いて電子透かしの埋め込みが行うことができる。

【００９１】ステップＳ１０３では、見出しデータ部１６に埋め込んだものと同じ格納情報を付属データ部１５に格納する。配布されたデジタルコンテンツを管理するサーバのURLと、見出しデータ部１６に埋め込まれた格納情報および付属データ部１５に格納されている格納情報とを検証すれば、デジタルコンテンツが正常に利用されていることを確認することができる。

【００９２】ステップＳ１１１では、デジタルコンテンツを管理するサーバの記録場所情報を取得する。ステップＳ１１２では、見出しデータ部１６に埋め込まれている格納情報を抽出する。この場合、前述したような見出しデータ部１６に対応する埋め込みロジックを用いて格納情報を抽出する。

【００９３】ステップＳ１１３では、付属データ部１７に格納されている格納情報を抽出する。ステップＳ１１４では、サーバの格納情報、見出しデータ部１６から抽出した格納情報および付属データ部１７から抽出した格納情報を比較して、同じ値であるか否かを検証する。

【００９４】このように構成した場合、見出しデータ部１６、実データ部１５および付属データ部１７を分離して不正利用しても、各格納情報を比較して検証することで不正利用を発見することが可能である。また、見出しデータ部１６に埋め込まれた格納情報と、付属データ部１７に格納された格納情報とを同じように置き換えたとしても、デジタルコンテンツを管理しているサーバの格納情報と比較して検証しているため、不正利用を発見することが可能となる。

【００９５】〔セキュリティ要求と画質要求〕画像データであるデジタルコンテンツ内に電子透かしを埋め込む場合には、ある程度画質が劣化することが問題となる。したがって、高画質が求められるようなデジタルコンテンツについては、可視的な電子透かしを埋め込むことが考えられる。また、セキュリティ要求が低いデジタルコンテンツについては、暗号化する必要もない場合がある。このような画質要求とセキュリティ要求とに基づいて、電子透かしの形態と暗号化の有無を各デジタルコンテンツについて設定することが可能である。

【００９６】デジタルコンテンツを合成データ１２内のデータとして取り込む際に、画質要求とセキュリティ要求に基づいて実データ部１５を作成する方法を図１９のフローチャートに基づいて説明する。

【００９７】ステップＳ１２１では、画質要求情報とセキュリティ要求情報とを入力する。たとえば、図２０に示すように、画質要求情報およびセキュリティ要求情報を、それぞれ"LOW"および"HIGH"とし、この組み合わせにしたがって、電子透かしの形態および暗号化の有無を設定するように構成できる。

【００９８】ステップＳ１２２では、入力された画質要求情報とセキュリティ要求情報に基づいて、図２０のテーブルを参照し、電子透かしの形態と暗号化の有無を決定して実データ部１５の生成を実行する。

【００９９】この場合、画質要求が高いデジタルコンテンツについては、不可視な電子透かしを用いずに画質の劣化を防止することが可能となる。著作権情報や版権に関する情報などについては、可視的な透かしとして埋め込むように構成しているため、不正な利用を防止することが可能となる。

【０１００】また、セキュリティ要求の高いデジタルコンテンツについてはコンテンツ鍵を用いた暗号化を行っており、セキュリティ効果を維持することができ、セキュリティ要求の低いデジタルコンテンツについては暗号化を省略することで、配布時における合成データ作成の時間の短縮および利用時における起動時間の短縮を図ることが可能となる。

【０１０１】〔他の実施形態〕

（Ａ）コンテンツ管理者２または他の特定の連絡先情報を見出しデータ部１６内に電子透かしと埋め込んだ構成とすることができる。この場合、ユーザ側で合成データ１２内のデジタルコンテンツを利用する際に、見出しデータ部１６から抽出した連絡先に回線接続を行い、コンテンツ情報を送出するように構成できる。

【０１０２】このことで、配布されたデジタルコンテンツの利用状況をコンテンツ管理者２側で監視することができ、不正利用を防止することが可能となる。

（Ｂ）合成データ１２中に含まれるデジタルコンテンツ１１の内容を代表するようなサンプルデータを抽出し、このサンプルデータを見出しデータ部とすることが可能である。

【０１０３】たとえば、デジタルコンテンツ１１が画像データを含む構成である場合に、このうち代表的な画像データを抽出し、この画像データに前述したような許諾情報１３を埋め込んで許諾情報付見出しデータ部１６を作成することが可能である。

【０１０４】デジタルコンテンツ１１が音楽データや音声データである場合には、その一部をサンプリングして、デジタルコンテンツの内容がわかるように構成することができる。

【０１０５】さらに、各デジタルコンテンツのタイトルや要約を読み上げた音声データを用いることも可能であり、この場合は、音楽データであるデジタルコンテンツの一部をサンプリングして見出しデータ部とする場合と同様に取り扱うことが可能である。

〔付記項〕

（付記１）配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化した

シンボル情報を備える見出しデータ部を作成し、前記デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

（付記２）前記見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその内容を視覚的に認識できるようにシンボル化された１つ以上の画像シンボルデータを、１つの画像データ内に合成してなる、付記１に記載のデータ運用方法。

（付記３）配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成する際に前記付属データ部を同時に合成して合成データを作成してこれを配布するデータ運用方法。

（付記４）前記利用制限情報は、前記許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックである、付記３に記載のデータ運用方法。

（付記５）前記利用制限情報は、前記デジタルコンテンツを利用可能な利用期限または利用回数に基づく、付記３に記載のデータ運用方法。

（付記６）前記利用制限情報は、前記デジタルコンテンツの利用者の個人情報を暗号鍵として暗号化されている、付記３～５のいずれかに記載のデータ運用方法。

（付記７）前記利用制限情報を暗号化する際の暗号鍵は、前記利用者によって予め設定されたパスワードである、付記６記載のデータ運用方法。

（付記８）前記利用制限情報を暗号化する際の暗号鍵は、前記合成データが記録される記録媒体に固有の識別情報である、付記６に記載のデータ運用方法。

（付記９）前記利用制限情報を暗号化する際の暗号鍵は、前記利用者の生体情報である、付記６に記載のデータ運用方法。

（付記１０）配布を行うデジタルコンテンツを暗号化した実データ部と、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部に、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部と、を合成して配布される合成データから付属データ部を分離し、前記付属データ部を復号化して利用制限情報を取り出し、前記利用制限情報に基づいて前記許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、前記許諾情報から前記デジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用者に利用させるデータ運用方法。

（付記１１）配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部からハッシュ関数を用いて生成されたハッシュ値を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこの合成データを配布することを特徴とするデータ運用方法。

（付記１２）配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、記録される記録媒体に固有の識別情報とを視覚的または聴覚的に認識不能な電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布することを特徴とするデータ運用方法。

（付記１３）配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、前記デジタルコンテンツを再生するための情報機器に特定の動作をさせる制御コードとを視覚的または聴覚的に認識不能な電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布することを特徴とするデータ運用方法。

（付記１４）配布を行うデジタルコンテンツを暗号化した実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識

不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、前記デジタルコンテンツのコンテンツ情報と、前記所定の連絡先情報とを、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成し、この合成データを配布することを特徴とするデータ運用方法。

（付記１５）配布を行うデジタルコンテンツを暗号化した実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部を合成した合成データを作成する際に、前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

（付記１６）前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、付記１５に記載のデータ運用方法。

（付記１７）配布を行うデジタルコンテンツを暗号化した実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部を合成して合成データを作成する際に、前記デジタルコンテンツの利用者の生体情報に基づいて生成された生体テンプレート情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

（付記１８）前記生体テンプレート情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、付記１７に記載のデータ運用方法。

（付記１９）配布を行うデジタルコンテンツを暗号化した実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部を合成して合成データを作成し、この合成データを配布するデータ運用方法であって、前記デジタルコンテンツの著作権情報や版権情報を含む権利情報を、前記デジタルコンテンツ中に電子透かしとして埋め込むことを特徴とするデータ運用方法。

（付記２０）前記デジタルコンテンツに要求されるデータ品質レベルとセキュリティレベルとに基づいて、前記デジタルコンテンツ中に埋め込む電子透かしの形態と暗号化レベルを決定することを特徴とする、付記１９に記載のデータ運用方法。

（付記２１）前記デジタルコンテンツ中への電子透かしの埋め込み方式と、前記見出しデータ部への電子透かしの埋め込み方式が、異なることを特徴とする、付記１９または２０に記載のデータ運用方法。

【０１０６】

【発明の効果】本発明では、デジタルコンテンツを暗号化して配布を行う際に、添付されている見出しデータ部のシンボル情報によりその内容を認識することが容易である。したがって、配布されるデジタルコンテンツのセキュリティを高く維持することが可能であるとともに、復号化する前にどのようなデジタルコンテンツが含まれているかを確認することが可能となる。

【０１０７】また、デジタルコンテンツを暗号化する際に用いたコンテンツ鍵の情報を含む許諾情報を見出しデータ部に電子透かしとして埋め込んであるため、コンテンツ鍵を別途管理する必要がなく、コンテンツ鍵を紛失して再発行を受けるような手間を省くことが可能となる。このコンテンツ鍵は、ユーザの指紋情報やパスワード、使用している情報機器の識別情報などを用いて暗号化することによって、正当なユーザにのみ復号化することが可能となり、不正使用を防止することができる。

【図面の簡単な説明】

【図１】本発明の概略構成を示すブロック図。

【図２】データ構造の一例を示す説明図。

【図３】データ構造の他の例を示す説明図。

【図４】コンテンツ管理者の制御ブロック図。

【図５】コンテンツ利用者の制御ブロック図。

【図６】制御の概略を示すフローチャート。

【図７】制御の概略を示すフローチャート。

【図８】シンボル情報とその種別および拡張子の対応を示すテーブル説明図。

【図９】認証用の指紋情報を合成データ中に記録する際の制御フローチャート。

【図１０】指紋情報により本人認証を行う際の制御フローチャート。

【図１１】実データ部への指紋情報を埋め込む際の制御フローチャート。

【図１２】電子透かし埋め込みロジックに関する情報を合成データ中に含ませる際の制御フローチャート。

【図１３】合成データ中の記録された電子透かし埋め込みロジックを用いて情報を取り出す際の制御フローチャート。

【図１４】電子透かし埋め込みロジックに関する情報の一例を示すテーブル説明図。

【図１５】実データ部のハッシュ値を見出しデータに埋め込む際の制御フローチャート。

【図１６】実データ部のハッシュ値によりデータ中の不正の有無を検証する際の制御フローチャート。

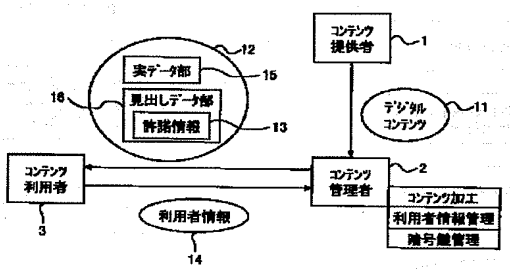
【図１７】デジタルコンテンツの管理サーバの記録場所に関する情報を合成データ中に記録する際の制御フロー＊チャート。

【図１８】デジタルコンテンツの管理サーバの記録場所に関する情報を用いて不正の有無を検証する際の制御フローチャート。

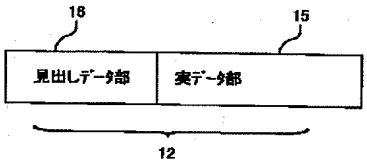
【図１９】画質要求情報とセキュリティ要求情報に基づいて実データ部の生成方法を決定する際の制御フローチャート。

【図２０】画質要求情報とセキュリティ要求情報に基づいて実データ部の生成方法を決定する際に用いるテーブルの説明図。

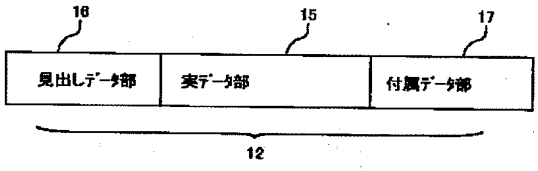
【図１】



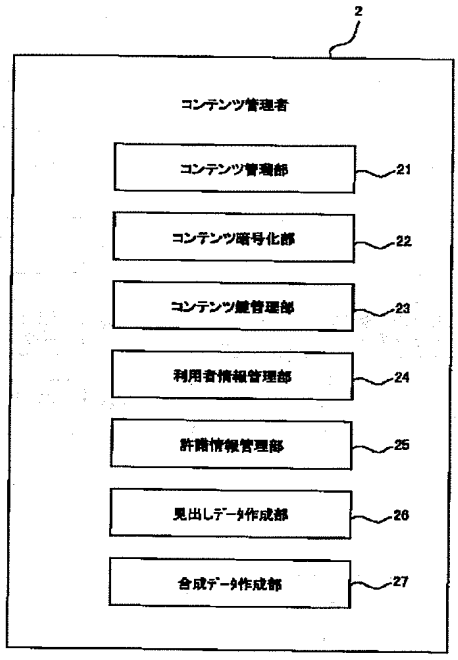
【図２】



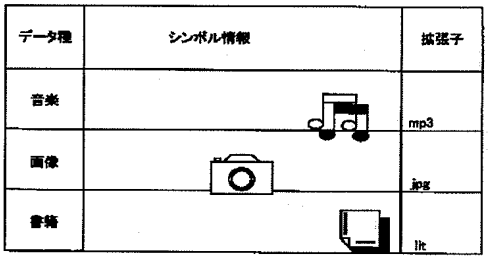
【図３】



【図４】



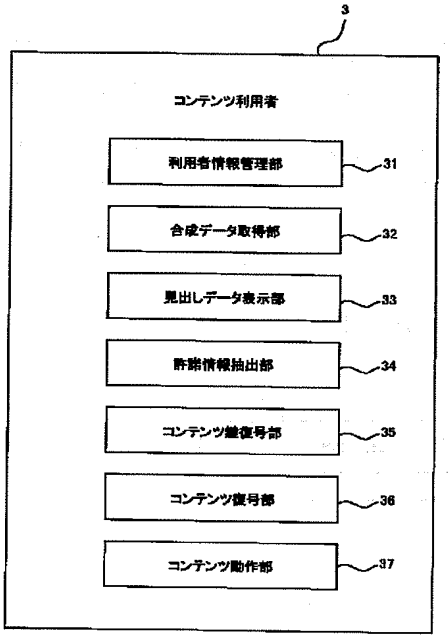
【図８】



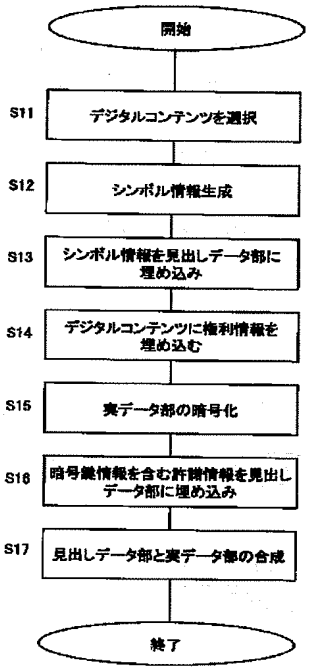
【図１４】

透かし埋め込み種別	見出しデータ部	実データ部
1111	Type1-Version1	Type1-Version1
2111	Type2-Version1	Type1-Version1
1100	Type1-Version1	――――

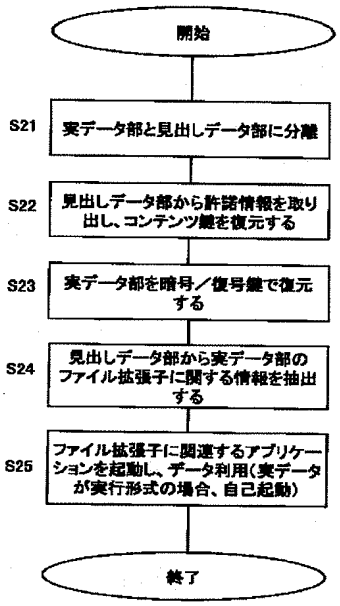
【図５】



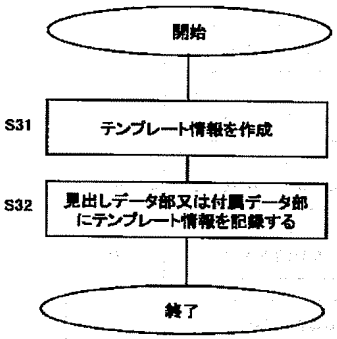
【図６】



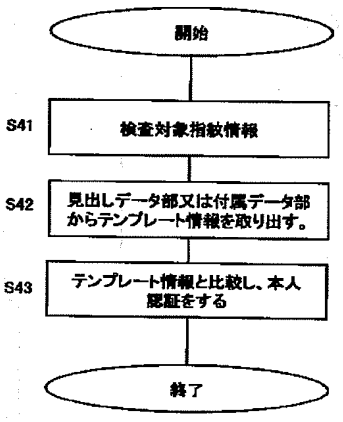
【図７】



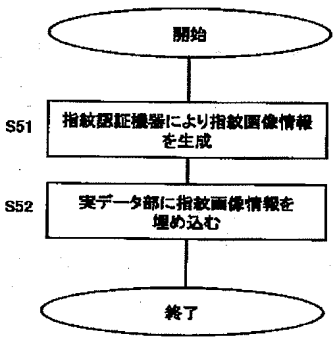
【図９】



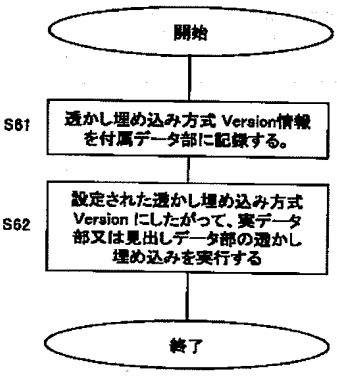
【図１０】



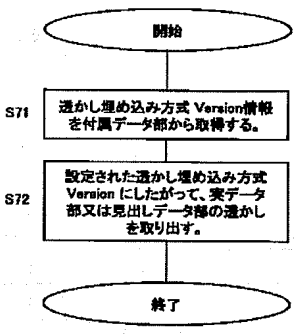
【図１１】



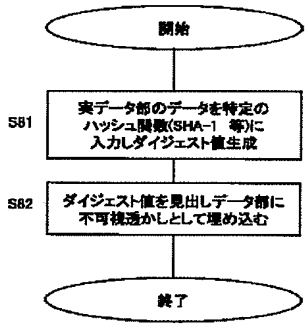
【図１２】



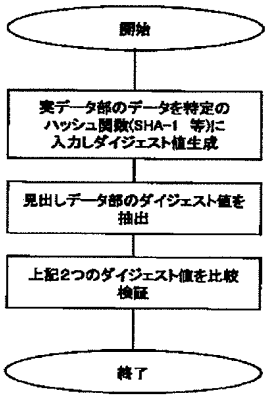
【図１３】



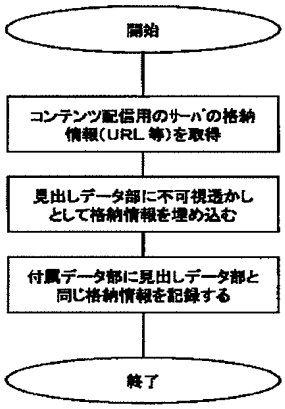
【図１５】



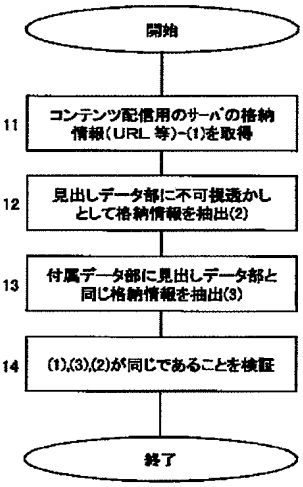
【図１６】



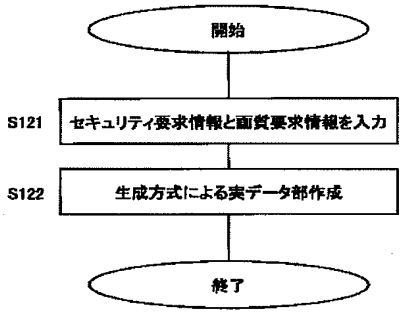
【図１７】



【図１８】



【図１９】



【図２０】

画質要求	セキュリティ要求	実データ部の生成例
Low	Low	不可視透かし，暗号化無
Low	High	不可視透かし，暗号化有
High	Low	透かし不要，暗号化無
High	High	可視透かし，暗号化有

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｇ１０Ｌ	19/00	Ｇ１０Ｌ	9/00	Ｅ
				Ｎ
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１Ｃ
Ｈ０４Ｎ	7/08	Ｈ０４Ｎ	7/08	Ｚ
	7/081			
	7/16			

(72)発明者　服部　衛紀
静岡県静岡市南町18番１号　株式会社富士通静岡エンジニアリング内
(72)発明者　望月　重利
静岡県静岡市南町18番１号　株式会社富士通静岡エンジニアリング内

Ｆターム(参考)　5B057 AA11 CE08 CG07
5C063 AB09 AC02 AC05 CA23 CA31 CA36 DA07 DB09
5C064 BA01 BB02 BC17 BC22 BC25 BC27 BD02 BD07 BD09
5C076 AA14 BA05 BA06
5J104 AA07 AA14 EA04 EA17 KA01 KA17 KA18 KA19 NA02 NA12